venminder

THE DIFFERENCES BETWEEN A HIGH-RISK AND CRITICAL VENDOR

As a best practice, there's a different definition and, therefore, **real differences** between a **high-risk vendor** and a **critical vendor**. This isn't something we've made up – this is something we've seen in the industry, heard at conferences, codified into programs at different organizations and executed effectively which has in turn been given good feedback in speaking with compliance officers and examiners.

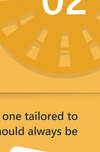
2 DIVISIONS OF RISKS

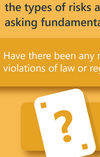
The differences between "HIGH RISK" and "CRITICAL" come down to two fundamental risks.

BUSINESS IMPACT RISK 01

The risk associated with whether you're so reliant on a third party, that if that third party were to suddenly disappear, it would cause a material disruption to your business. If you believe that's the case, then that's a critical third party.

You may have a vendor who is CRITICAL BUT LOW RISK. Think of the phone company.





You could have a vendor who is NON-CRITICAL BUT HIGH-RISK. Think of the shred vendor.

They can be replaced easily, but in the case of the shred vendor, THEY'RE LITERALLY WALKING OUT THE DOOR WITH **YOUR** DATA!

REGULATORY RISK 02

Working your way through the various categories of risk laid out in the guidance. For example, FDIC FIL-44-2008 and OCC Bulletins 2013-29 and 2017-7 identify numerous categories of risk you should consider.

Whether you use a standardized questionnaire or one tailored to the types of risks associated with a vendor, you should always be asking fundamental questions such as:

Have there been any reported/disclosed violations of law or regulatory guidance?

Are all policies and procedures reviewed and approved on an annual basis?

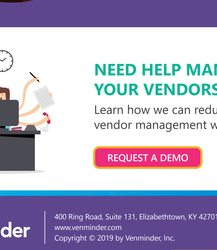
Are all materials, terms and conditions required to have the organization's review and approval prior to distribution by the vendor?

Does the vendor process transactions on behalf of your organization, customers or employees?

Is sensitive data, such as nonpublic information (NPI) or personally identifiable information (PII), being exchanged?

Of course, these will vary depending on whether it's your marketing vendor or your shred vendor, but you should develop a set of questions that help you fully discern the risk.

There are many categories of risk that may come into play, depending on the type of product or service. The guidance referenced above lists a few, but you should consider if there are others in play as well.



Various risks cited in guidance include:

- ⚠ Strategic Risk
- ⚠ Financial Risk
- ⚠ Operational Risk
- ⚠ Reputational Risk
- ⚠ Transactional Risk
- ⚠ Compliance Risk

However, you may very well find you need to think about other risk such as:

- ⚠ Geographic Risk
- ⚠ Country Risk
- ⚠ Concentration Risk
- ⚠ Information Security Risk...

...just to name a few.

JUST TO RECAP

HERE ARE EXAMPLES OF HOW THIS WORKS

You could easily have a critical third party who is low risk.

Think of the phone vendor, if they fall within your scope.

You're absolutely reliant on them to be up and available and their disruption would impact your activities and your customers, but there's very low risk associated with them from a regulatory risk perspective.

Conversely, you could have a non-critical third party who is high risk.

Think of your shred vendor or your backup server provider.

You could likely do without them for a day or replace them in relatively short order, but they have unfettered access to all of your confidential information and your customer data.

NEED HELP MANAGING YOUR VENDORS?

Learn how we can reduce your vendor management workload.

REQUEST A DEMO

venminder

400 Ring Road, Suite 131, Elizabethtown, KY 42701 | (270) 506-5140
www.venminder.com

PRINTABLE VERSION